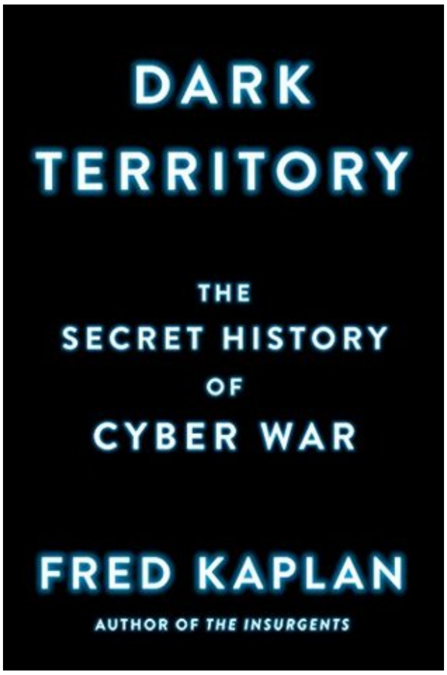

Dark Territory: The Secret History of Cyber War

Fred Kaplan

Dark Territory: The Secret History of Cyber War

Fred Kaplan

Dark Territory: The Secret History of Cyber War Fred Kaplan
“A consistently eye-opening history...not just a page-turner but consistently surprising.” —*The New York Times*

“A book that grips, informs, and alarms, finely researched and lucidly related.” —John le Carré

As cyber-attacks dominate front-page news, as hackers join terrorists on the list of global threats, and as top generals warn of a coming cyber war, few books are more timely and enlightening than *Dark Territory: The Secret History of Cyber War*, by *Slate* columnist and Pulitzer Prize–winning journalist Fred Kaplan.

Kaplan probes the inner corridors of the National Security Agency, the beyond-top-secret cyber units in the Pentagon, the "information warfare" squads of the military services, and the national security debates in the White House, to tell this never-before-told story of the officers, policymakers, scientists, and spies who devised this new form of warfare and who have been planning—and (more often than people know) fighting—these wars for decades.

From the 1991 Gulf War to conflicts in Haiti, Serbia, Syria, the former Soviet republics, Iraq, and Iran, where cyber warfare played a significant role, *Dark Territory* chronicles, in fascinating detail, a little-known past that shines an unsettling light on our future.

Dark Territory: The Secret History of Cyber War Details

Date	:	Published March 1st 2016 by Simon & Schuster
ISBN	:	
Author	:	Fred Kaplan
Format	:	Kindle Edition 353 pages
Genre	:	Nonfiction, History, Science, Technology, Politics, War

Download Dark Territory: The Secret History of Cyber War ...pdf

Read Online Dark Territory: The Secret History of Cyber War ...pdf

Download and Read Free Online Dark Territory: The Secret History of Cyber War Fred Kaplan

From Reader Review Dark Territory: The Secret History of Cyber War for online ebook

Peter Mcloughlin says

Covers the history of cyber security and cyber warfare in the US from the 1980s through Obama's tenure. This might be related to another book called "the seventh sense." Power now is defined as the ability to hack and control network platforms. The ability to do so gives hackers and hacking organizations supreme power over power grids, weapon systems and just about anything hooked up to a computer network nowadays. Mastery of this technology which easier to offensively wield than play defense is key for our safety and power. This puts control of our lives in a very small group of hackers who now decide fates of nations (witness the 2016 US election). These trends put power in few hands. Computers once thought a tool of democracy is, in fact, a powerful tool for narrowing elite over the majority of the world's people.

John Lamb says

I continue my quest to be the most informed snob at any dinner party so I can maintain my delicate card tower of affected pretentiousness by finishing this book about America's secret war of cyber attacks. I will let you know know the most interesting bits in person.

Derkanus says

Summary: Dark Territory covers the history of US cyber security in fairly broad strokes. These are some of the major events that it discusses:

NSDD-145: After seeing the movie "Wargames" and learning that the state of US cyber security was actually WORSE than it was portrayed in the movie, President Reagan signed this directive that provided initial objectives, policies, and an organizational structure to guide the conduct of federal activities toward "safeguarding systems which process or communicate sensitive information from hostile exploitation," and established a high-level interagency group to implement the new policy. It gave leading roles to the National Security Council, DoD, and NSA.

Eligible Receiver: A U.S. government exercise conducted under what is known as the No-Notice Interoperability Exercise Program, in 1997. The NSA Red Team used hacker techniques and software that was freely available on the Internet at that time and were able to crack networks and do things such as deny services; change and manipulate emails to make them appear to come from a legitimate source; disrupt communications between the National Command Authority, intelligence agencies, and military commands. Common vulnerabilities were exploited which allowed the Red Team to gain root access to over 36 government networks which allowed them to change/add user accounts and reformat server hard drives. They gave themselves 2 weeks as a goal, but accomplished it in 4 days.

Solar Sunrise: Using a computer virus, hackers in 1998 penetrated and took control of over 500 computer systems that belonged to the army, government, and private sector of the United States. They also inserted malware into the computers. The whole situation was dubbed "Solar Sunrise" after the popular vulnerabilities in computers that ran on operating systems called SunSolaris. Initially, it was believed that the attacks were planned by operators in Iraq. It was later revealed that the incidents represented the work of two American teenagers from California.

Moonlight Maze: In 1999, a coordinated attack on an unprecedented scale was unleashed by attackers proxying through University networks and small businesses. The attackers used standard tools (Telnet and FTP) to move through networks and steal documents without standing out. The attacks were traced to Russia, and the FBI worked with a Russian General over there who insisted he'd help trace the attacks. A few days in, he disappeared and was never heard from again.

Buckshot Yankee: A 2008 cyberattack on the United States that was the "worst breach of U.S. military computers in history". The defense against the attack was named "Operation Buckshot Yankee". It led to the creation of the United States Cyber Command. It started when a USB flash drive infected by a foreign intelligence agency was left in the parking lot of a Department of Defense facility at a base in the Middle East. It contained malicious code and was put into a USB port from a laptop computer that was attached to United States Central Command. From there it spread undetected to other systems, both classified and unclassified. The Pentagon spent nearly 14 months cleaning the worm, named agent.btz, from military networks. Agent.btz has the ability "to scan computers for data, open backdoors, and send through those backdoors to a remote command and control server." It was suspected that Russian hackers were behind it because they had used the same code that made up agent.btz before in previous attacks. In order to try and stop the spread of the worm, the Pentagon banned USB drives, and disabled Windows autorun feature.

Aurora Generator Test: This demonstrated how a cyber attack could destroy physical components of the electric grid. The experiment used a computer program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid and cause it to explode.

Stuxnet: A malicious computer worm that targets industrial computer systems; was responsible for causing substantial damage to Iran's nuclear program. Although neither country has admitted responsibility, the worm is now generally acknowledged to be a jointly built American-Israeli cyberweapon. It specifically targets PLCs, which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet went beyond its intended scope and spread outside of the Iranian computers, which was how it was discovered and traced back to the US.

China Unit 61398: The Military Unit Cover Designator of a People's Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks. They stole from the government and businesses.

DarkSeoul: In 2013, three South Korean television stations and a bank suffered from frozen computer terminals in a suspected act of cyberwarfare; ATMs and mobile payments were also affected. North Korea has been blamed for similar attacks in 2009 and 2011 and was suspected of launching this attack as well.

Five Guys Report: After the Snowden leaks, Obama threw together a group of 5 non-government personnel to determine what the government should do to fix people's worries about the government collecting their data. They came up with a report to develop deterrence strategies and programs, take the data from the NSA and keep it with the phone companies, etc.

Review: 3.5 stars. There was a lot of stuff covered in this book, but it was all very abstract. It also focused too much on the people behind everything, and I found it hard to keep track of all of them (and didn't really care about them either).

It was worth reading just to see how incredibly terrible our military handled cyber security all the way up until like 2015. It seemed like there was practically nothing in place to handle cyber attacks until Obama got into office; the NSA just did whatever they wanted, collected every bit of data from every network (though it was only considered "collected" if they accessed it later on), etc.

Radiantflux says

49th book for 2017.

An interesting history of cyberwarfare over the last 50 years, almost exclusively told from an American perspective.

The big take home messages for me were: how vulnerable societies (and interestingly in particular the US) are from crippling attacks (from power stations to hospitals to voting systems); how concerted, long-term lobbying pressure from Silicon Valley has left huge gaps in security, which is almost a design feature as costs of attacks are externalized on society as a whole; how the military (and politicians) continue to have trouble understanding the damages of cyberattacks, despite decades of warnings, even those coming from Presidential Commissions - blowing things up is so much easier to understand; how the temptation to eavesdrop on US domestic communications is so high, given that 80% of the World's internet traffic flows through the US - in fact almost all from through a few buildings in downtown New York and a couple of other US cities; and finally, and most interesting, how the NSA is perhaps not as bad as everyone thinks (I need to digest that last one a bit more).

Unfortunately, I found the writing style quite bland; not doing full justice to a very interesting and important story.

David Sasaki says

My instinct is to ignore the warnings of lawyers, security experts, and anyone else whose income is based on their capacity to invoke fear. With hindsight, it's an instinct that has served me well; the long arc of history is usually on the side of the optimists. But it is also my blindspot. Rarely to I seek out information about the risks and dangers we face.

Fortunately, my colleague Eli Sugarman suggested that we read Fred Kaplan's *Dark Territory: The Secret History of Cyber War* as the first installment for our Hewlett Foundation nonfiction book club. It was a timely read; cyber warfare has become one of the biggest policy issues of the campaign, and each day brings increasingly dystopian headlines about cyberhacks that erode our trust in our devices, our presumed privacy, and our democracy. First, Trump insinuates that Russian hackers should break into Clinton's email, and then hacker magazine *2600* offers a $10,000 bounty to any hacker able to uncover Trump's tax returns. Meanwhile, the US Department of Homeland Security is begging state election authorities to seek help to secure their voting systems against cyberattacks.

I'm the kind of person who learns about the complexities of contemporary issues by studying their history, and so Kaplan's historical telling of the rise of cyber war and the institutions created in response served me well. I had no idea, for example, that the National Security Agency has its roots in World War I, when the government created "MI-8" to surveil all incoming telegraphs from Europe. It continued to do so for ten years after the end of the war until Secretary of State Henry Stimson finally shuttered the program in 1929, proclaiming, "Gentlemen don't read each other's mail."

A game of cat and mouse resurfaces with each historical anecdote. The US government -- usually the NSA -- discovers some exploitation with which it can surveil its enemies, but also realizes that we are equally susceptible to the same exploitation by others. We were able to penetrate the nuclear reactors of Iran (which were run on Microsoft Windows!), and yet much of our national infrastructure is just as susceptible to attack. Over the years the NSA regularly assembles teams of internal hackers and sets them loose to see how much damage they could hypothetically inflict. A lot, it turns out, and each exercise in exploitation is an effective strategy to request billions from Congress for another expensive policy effort to bolster defense of national cyber-security. Most of the vulnerabilities, however, are embedded in commercial software like Windows, and the private sector has little incentive to invest costly resources in security and cryptography, which tends to slow down performance and means little to consumers that have grown accustomed to free software with new features. When the NSA does uncover vulnerabilities in commercial software, they have to balance the opportunity of using them to break into the computers of terrorists with the risk of terrorists and foreign governments using them to exploit American interests.

The book was also a helpful corrective to my superficial understanding of the NSA's PRISM surveillance program famously disclosed by Edward Snowden. The initial reporting and media fallout over PRISM didn't give readers historical context about the NSA's longstanding relationship with software companies even before the PRISM program. I was under the impression that it was the NSA pressing companies like Microsoft to create backdoors that would allow for surveillance, when it fact it was more often the NSA alerting Microsoft that there were vulnerabilities that allowed *anyone* to gain access to users' data. Snowden's leaks were fundamental to alerting the public to the *potential* for abuse (I certainly wouldn't entrust PRISM to a Trump administration), but it's amazing how thoughtful and restrained the NSA actually was in its pursuit of information related to terrorists with little legislation in place to force oversight.

Fortunately, Snowden's leaks prompted Obama to create a five-person commission to draft a report and policy recommendations to better balance "liberty and security in a changing world." Kaplan's chapter describing the relationships and interactions between these five old white guys with gigantic egos is among the most entertaining of the book. They were chosen intentionally for their diverse viewpoints, and yet all five men came to complete agreement about the changes needed to establish sufficient oversight of surveillance in the name of security and protection from surveillance in the name of liberty. Their recommendations prompted by Snowden's leaks led to a number of important reforms, but Obama chose not to adopt all the recommendations, which makes one think that he's seen firsthand the importance of data collection in deterring attacks.

This book is a must-read for anyone who assumes that the NSA does little more than infringe on our civil liberties. Our culture celebrates those who respond heroically during disaster (think the firefighters of 9/11), but does little to recognize those who prevent disasters from happening in the first place (think of a hypothetical engineer who had invented a way of securing cockpits so the 9/11 terrorists couldn't have broken in).

I would have appreciated a final chapter from Kaplan speculating on the future of liberty, security and cyberwar. It seems inevitable that the game of privacy cat and mouse will continue until the computers themselves become better at creating and cracking cryptography than the humans that once programmed them. The cryptography we use today to secure our email, financial transactions and most private documents will be rendered obsolete by quantum computers. Driverless cars, wireless credit cards, instant cloud storage of everything, smart homes -- the more we connect the more vulnerable we become. My biggest takeaway from the book is that there is real reason for concern, and that the NSA is pretty low down on the list of what we should be concerned about.

Though 2016 has seemed like a year of death and disaster, in fact it's been one of the most peaceful years in the history of our species. We've come to take it for granted that major wars between nation states is seemingly a phenomenon of the past. And yet moving forward, cyberwarfare between countries and groups within countries is set to become a constant.

Lynda says

Interesting, but not well written.

Andrew Obrigewitsch says

An excellent history of cyber warfare. One can see how this could easily escalate out of control, and is the weapon of the future which most companies aren't even thinking about defending against. Which puts them at grave risk.

Karel Baloun says

We are at a dramatic crux in military strategy, where cyber warfare is becoming perhaps the most active battle ground. China is actively penetrating systems, and Russia is leading in information warfare. The first chapters feel historical, even when relating events from just 10-20 years ago, yet the conclusion couldn’t possibly be more timely or more imminently impactful. Well researched and carefully written. Powerful.

This book inspired me to go study for a masters in cybersecurity.

Valuable perspective on Snowden: He was not just the simple libertarian anti-military folk hero, as some lobbied for his pardon by Obama. The debate about NSA operations is SO MUCH MORE than a focus just domestic surveillance. He released Tailored Access Operations (TAO) inventory of exploits and tools, and this greatly aided cyber criminal activity.

This is a hard book to read and then forget. We are asymmetrically vulnerable to cyber attacks, both on our basic civilian infrastructure and on our modernization and progress to comfort. Our society is so far from anti-fragile.

The public doesn’t understand even a tiny sliver of what is necessary for democratic participation. As with climate change, we lack all sense of crisis and vulnerability.

Ross Siegel says

Fascinating and scary read about the state Of modern warfare

Kaplan does a spectacular job about laying out the facts of the history of American warfare and the people and events that drove policy or lack thereof.
The world is scarier now which is why it's more important that everyone with an eye to government over reach, foreign policy, freedom of information and privacy read this book.
I do wish, however that Kaplan had spent more time discussing what America does in a modern offensive stance rather than a focus on the defensive. I know a lot now about the threats to America but far less about what we do to deter cyber warfare by using tactics against would be intruders.

John de' Medici says

Found this to be an highly engrossing read, especially because I have for a time been keen on the topic of "cyber warfare"...
I especially loved this book's approach - a behind the scenes look into the History of Cyber War in relation to the US. The NSA of course taking the major spotlight.

Any good book I think should be able to make you reconsider one or more viewpoints that you hold...
This too was no exception. I find myself reconsidering my attitude towards the NSA, much of it formed during the somewhat recent scandal.

Barbara (The Bibliophage) says

This is compelling book about a worldwide issue that's underreported, under addressed, and honestly terrifying. Governments have been hacking into their rivals' computers for decades but it's taken nearly as long for cyber attacks to be considered a genuine threat.

This also could have a real snoozer of a book, given the complexity of the topic. But Kaplan and the audiobook narrator (Malcolm Hillgartner) make it easier to understand than I expected. That said, I could probably gain even more insight (and recall of facts) by listening a second time. But maybe that's just me and my wandering attention span.

Kaplan lays out the bureaucratic infighting and ignorance that delayed the viability of both offensive and defensive cyber warfare. He explains the background and motivations of the major players, including Presidents since Reagan. In addition, he explains the vulnerabilities of commerce, power, government, and Internet systems on a national and international scale.

If I could wish for one thing, it would be to hear what he thinks of the developments in the years since the book's publication.

I highly recommend this for techies, political junkies, and regular folks.

Bettie? says

Description: *In June 1983, President Reagan watched the movie War Games, in which a kid unwittingly hacks the Pentagon, and asked his top general if the scenario was plausible. The general said it was. This set in motion the first presidential directive on computer security.*

The first use of cyber techniques in battle occurred in George H.W. Bush's Kuwait invasion in 1991 to disable Saddam's military communications. One year later, the NSA Director watched Sneakers, in which one of the characters says wars will soon be decided not by bullets or bombs but by information. The NSA and the Pentagon have been rowing over control of cyber weapons ever since.

From the 1994 (aborted) US invasion of Haiti, when the plan was to neutralize Haitian air-defenses by making all the telephones in Haiti busy at the same time, to Obama's Defense Department 2015 report on cyber policy that spells out the lead role played by our offensive operation, Fred Kaplan tells the story of the NSA and the Pentagon as they explore, exploit, fight, and defend the US. Dark Territory reveals all the details, including the 1998 incident when someone hacked into major US military commands and it wasn't Iraq, but two teenagers from California; how Israeli jets bomb a nuclear reactor in Syria in 2007 by hacking into Syrian air-defense radar system; the time in 2014 when North Korea hacks Sony's networks to pressure the studio to cancel a major Hollywood blockbuster; and many more. Dark Territory is the most urgent and controversial topic in national defense policy.

Surprise!

Kathrin says

Good recounting of the development of the perception of cyber treats from the Reagan to the Obama presidency and how the executive branch reacted to the rapid change of information warfare. Still, the writing (or the narration) left me very disengaged.

Jason says

A better title would have been "Dark Territory: A History of American Cyber Security Bureaucracy."

This book contains a wealth of information and a number of interesting stories and insights. Unfortunately, it is a laborious and nod-off inducing read, by a well informed author with no clue how to build a compelling narrative or meaningful critical perspective. It also places far too much emphasis on the bureaucracies of the American defense complex and not enough emphasis on the larger scope of the titular topic.

Mal Warwick says

Occasionally, I come across a book on an important topic that's crammed with information I was able to find nowhere else — but is a chore to read. Even though it is not an academic study but clearly intended for a general audience, Fred Kaplan's recent history of cyber war, Dark Territory, is one such book.

A story stretching over five decades

Unlike previous treatments that I've read about the topic, which zero in on the vulnerability of the American economy to attacks through cyberspace, Dark Territory traces the history of our government's slowly growing awareness of the threat, beginning nearly half a century ago. Then, a prescient Pentagon scientist wrote a paper warning about the dangers inherent in computer networks. Apparently, though, no one in a position to do anything about it paid much attention to him.

Kaplan identifies an incident fully fifteen years later in 1984 when President Ronald Reagan — a movie fan, of course — saw the film War Games. He queried the chairman of the Joint Chiefs of Staff at a top-level White House meeting whether it was possible for a teenager like the one portrayed in the film by Matthew Broderick to hack into sensitive Pentagon computers. When the chairman, General John Vessey, reported some time later that the feat was in fact possible, Reagan called for and later signed the government's first policy directive on the topic of cyber war. But that, too, led to no significant change at the Pentagon or anywhere else in the federal government.

Dark Territory is filled with revealing anecdotes like this, based on what surely was top-secret information not long ago. Kaplan reveals many little-known details about the Russian cyber war on Estonia and Ukraine, the Chinese Army's prodigious hacking of American corporations and the Pentagon, the massive North Korean assault on Sony, Iran's disabling of 20,000 computers in Sheldon Adelson's casino empire, and the successful US-Israeli attack on Iran's nuclear infrastructure. Kaplan also reveals the reason why US complaints about China's cyber attacks have fallen on deaf ears: it turns out that the National Security Agency is attacking the Chinese government in much the same way. As The Guardian revealed in 2013, "the NSA had launched more than 61,000 cyber operation, including attacks on hundreds of computers in Hong Kong and mainland China."

The book casts a particularly harsh light on the Administration of George W. Bush. Bush, Cheney, Rumsfeld, and other senior officials in the early 2000s cavalierly dismissed urgent reports from national security and intelligence officials that the threat of cyber war, and the vulnerability of the US economy, were growing at an alarming rate. Only under Bush's successor did reality strongly take hold. As Kaplan writes, "During Barack Obama's presidency, cyber warfare took off, emerging as one of the few sectors in the defense budget that soared while others stayed stagnant or declined."

It's difficult to understand how anyone who was awake could have failed to grasp the problem. For example, a war game conducted in 1997 was intended to test the vulnerability of the Pentagon's computer systems within two weeks. "But the game was over — the entire defense establishment's network was penetrated — in four days. The National Military Command Center — the facility that would transmit orders from the president of the United States in wartime — was hacked on the first day. And most of the officers manning those servers didn't even know they'd been hacked." Not long afterwards, the Pentagon was hacked in a similar way by two 16-year-old boys in San Francisco. And when national security officials widened the scope of their attention to encompass the country's critical civilian infrastructure, such as the electricity grid, they were shocked to discover that the situation was far worse. The Pentagon eventually bowed to the warnings and implemented needed security measures. But private corporations blatantly refused to do so because they didn't want to spend the money — and Congress declined to allow the federal government to make security measures obligatory.

Unfortunately, Kaplan's book is poorly organized. It's roughly structured along chronological lines but jumps back and forth through time with such regularity as to be dizzying. And it's crammed so full of the names of sometimes obscure government officials and military officers that it becomes even more difficult to follow the thread of the story.

However, these challenges aside, a picture clearly emerges from Dark Territory: For decades the American public has been at the mercy of incompetent and pigheaded people in sensitive positions in the government, the military, and private industry — and we still are. Bureaucratic games proliferate. Politics intrude. Inter-service rivalries abound. Personal grudges get in the way. Repeatedly, some of those who are entrusted with the security of the American people make what even at the time could easily be seen as stupid decisions.

Other takes on cyber war

Last year I read and reviewed a book titled Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It, by Marc Goodman. I described it as "the scariest book I've read in years."

Five years earlier, I read Cyber War: The Next Threat to National Security and What to Do About It, by Richard A. Clarke and Robert K. Knake. From the early 1970s until George W. Bush's invasion of Iraq, Clarke filled high-level national security positions under seven Presidents, so he knows whereof he writes. (He resigned in protest over the invasion of Iraq, which he thought distracted the government from the real threats facing the country.) Not long afterward, I read and reviewed Worm: The First Digital World War, by Mark Bowden, a much more focused treatment of the topic — a case study, really — but equally unsettling.

Though less current, all three of these books are better organized and more readable than Dark Territory. Admittedly, though, Kaplan's book reveals the history that is only hinted at in the others.

About the author

Fred Kaplan wrote five previous books about the nuclear arms race and other topics bearing on US national security. He was on a team at the Boston Globe in 1983 that won a Pulitzer Prize for a series about the nuclear arms race.